Inhalt

1. Zweck

Der „Informationssicherheitsleitfaden für Partnerfirmen“ definiert die Informationssicherheitsvorschriften, die von Partnerfirmen in ihrem Verantwortungsbereich für von ihnen bereitgestellte und genutzte IT-Systeme und -anwendungen und Infrastruktur zu berücksichtigen sind. Partnerfirmen müssen geltende Vorschriften beachten und einhalten.

In diesem Informationssicherheitsleitfaden werden die Regeln für Informationssicherheit definiert, die von Partnerfirmen beim Umgang mit Informationen und IT-Geräten (z.B. PCs, Arbeitsplätze, Laptops, Smartphones oder Tablet-PCs) einzuhalten sind.

Zweck des Informationssicherheitsleitfaden ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Schutz der Rechte und Interessen des Auftraggebers und aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit dem Auftraggeber eingehen und/oder Tätigkeiten für diesen ausführen.

Zur Einschätzung der Informationssicherheit hat die CleanControlling GmbH eine Informationsklassifizierung eingeführt. Jede externe Partei wird in Bezug ihrer Vertraulichkeit, Integrität und Verfügbarkeit bewertet und entsprechend der Einteilung wurde das weitere Vorgehen definiert.

2. Geltungsbereich

Der Handlungsleitfaden gilt für die Partnerfirmen der Fa. CleanControlling GmbH und CleanControlling Medical GmbH&Co.KG und sind im gesamten Partnernetzwerk für Partner, die auf Basis von vertraglichen Regelungen Leistungen für die genannten Firmen erbringen, anzuwenden und durch konkrete

organisatorische und technische Regelungen (z.B. IT Regelungen) im Einzelfall zu erarbeiten.
Die Anforderungen sind vom Lieferpartner an Unterauftragnehmer weiterzuleiten.

3. Umsetzung

Die beschriebenen Regeln sind für die Partnerfirmen eigenständig verpflichtend, sobald vom Auftraggeber, der CleanControlling GmbH und der CleanControlling Medical GmbH&Co.KG, als geheim bzw. vertraulich klassifizierte Informationen zugänglich gemacht werden.

Nicht gekennzeichnete Informationen sind als „nicht vertraulich“ zu behandeln.

Sollten einzelne Vorschriften in der aktuellen Situation nicht umsetzbar sein (z.B. technische Gründe), so ist wie folgt zu verfahren:

- der Umstand muss an die CleanControlling (Medical) GmbH gemeldet werden
- im Einzelfall muss sich jeder so verhalten, dass er dem eigentlichen Ziel und Zweck der Regelung möglichst nahekommt.

Bei zwingendem Bedarf können abweichende Ausnahmen schriftlich durch die CleanControlling (Medical) GmbH genehmigt werden.

4. Gültigkeit

Dieser Leitfaden ist unbefristet und unbeschränkt gültig.

5. Allgemeine Anforderungen

5.1. Organisatorische Anforderungen

Regelungen der CleanControlling (Medical) GmbH bezüglich des Mitbringens von externen IT-Geräten auf das Firmengelände oder in Sicherheitsbereiche müssen eingehalten werden.

Das Verwenden von Daten oder Software auf IT-Systemen oder Speichergeräten, die weder durch den Auftraggeber oder Dienstleister bereitgestellt oder freigegeben sind, ist nicht zulässig.

Die Weitergabe von Daten an Dritte kann nur unter Einhaltung dieses Leitfadens erfolgen und ist nur mit schriftlicher Freigabe vom Dateneigentümer gestattet. Eine bestehende Geheimhaltungsvereinbarung gilt als schriftliche Freigabe für den Datenaustausch.

Mitarbeiter des Dienstleisters müssen von ihrer Geschäftsleitung auf die Geheimhaltung im Sinne der bestehenden Vertraulichkeitsvereinbarung zwischen Auftraggeber und Auftragnehmer verpflichtet werden. Dem Auftraggeber ist jederzeit Einsicht in diese Vereinbarungen zu gewähren.

Falls Daten des Auftraggebers auf mobilen Systemen oder IT-Geräten gespeichert werden, sind diese mit dem aktuellen Stand der Technik entsprechender Hardware oder Software zu verschlüsseln.

Vor Auslandsreisen sind die länderspezifischen Regelungen zum Einsatz von Sicherheitstechniken (z.B. Verschlüsselung) zu beachten.

Nach Vertragsende müssen Daten des Auftraggebers an den Auftraggeber übergeben werden und sind auf Geräten und Speichermedien des Dienstleisters zu löschen oder nach aktuellem Stand der Technik sicher zu verwahren. Rechtliche Anforderungen (z.B. Aufbewahrungspflichten) sind zu beachten.

5.2. Personalsicherheit

Sofern ein Nutzer eine nicht mehr benötigte Benutzerkennung oder ein nicht mehr benötigtes Zugriffsrecht auf Daten des Auftraggebers hat, ist dies vom jeweiligen Nutzer unverzüglich bei einer verantwortlichen Stelle zu melden (z.B. Systemadministrator). Anschließend erfolgt eine sofortige Sperrung/Löschung. Grundsätzlich ist bei der Erteilung von Privilegien das Minimalprinzip anzuwenden.

Die im Zusammenhang eines Dienstleistungsvertrages überlassenen Geräte (z.B. Laptops) und Datenträger bzw. Speichermedien müssen nach Ablauf des Vertrags, oder wenn diese nicht mehr benötigt werden, an den Auftraggeber zurückgegeben werden.

5.3. Physische und umgebungsbezogene Sicherheit

IT-Geräte, die Daten der CleanControlling (Medical) GmbH speichern oder verarbeiten sind so zu verwenden, dass keine Unbefugten diese Daten einsehen oder darauf zugreifen können. Besondere Vorsicht ist bei der Verwendung mobiler Systeme geboten.

Grundsätzlich dürfen vertrauliche und geheime Dokumente niemals unbeaufsichtigt liegengelassen werden, um Einsichtnahme durch Unberechtigte zu verhindern.

5.4. Management von Werten

Im Rahmen der Informationssicherheit sind primär drei Schutzziele zu verfolgen:

- Vertraulichkeit
- Verfügbarkeit

- Integrität

Bei nicht eindeutiger Klassifikation hinsichtlich der Vertraulichkeit muss diese vom Auftragnehmer eingefordert werden. Informationen sind über ihre gesamte Lebensdauer hinweg gemäß den Maßnahmen, die ihrer Vertraulichkeitseinstufung entsprechen, vor unbefugtem Zugriff zu schützen.
Informationen dürfen nur einer berechtigten Gruppe von Personen zum Zwecke der vereinbarten Tätigkeiten und unter Einhaltung der entsprechenden Regelungen zugänglich gemacht werden.

5.5. Umgang mit Informationssicherheitsvorfällen

Informationssicherheitsvorfälle (z.B. auftretende Störungen, Verstöße gegen das Informationssicherheits-Regelwerk, Verlust von geheimen oder vertraulichen Informationen), welche Daten oder Systeme des Auftraggebers betreffen sind unverzüglich der nachfolgend benannten zuständigen Stelle zu melden:

security@cleancontrolling.de

Der Informationssicherheitsbeauftragte der CleanControlling GmbH entscheidet je nach Art des Vorfalls über die weitere Vorgehensweise und über die zu benachrichtigenden bzw. einzuschaltenden Stellen, z.B. fachverantwortliche Stellen, Personalabteilung, Datenschutzbeauftragter etc. Er leitet die erforderlichen Maßnahmen zur Schadensbegrenzung und zur Behebung der Störung ein.